LIST OF CURRENT CLAIMS

1. (Currently amended) A method for authenticating a user of a data carrier for authorized use of the data carrier and for authenticating a data carrier terminal for authorized accessing by the data carrier terminal of memory areas of the data carrier, comprising the following steps:

reading a secret code from the data carrier by the data carrier terminal, wherein the secret code is stored on a memory location that can be accessed only by authorized data terminals or can be decrypted correctly only by authorized data terminals;

presenting the read secret code to the user;

after receiving an indication by the user that the presented read secret code is correct, reading a biometric feature presented by the user;

comparing the read presented biometric feature with a biometric feature stored on the data carrier.

2. (Previously presented) A method according to claim 1, further comprising a step wherein a PIN is in addition presented to the terminal and compared with a PIN stored on the data carrier.

3. (Previously presented) A method according to claim 1 or 2, wherein a finger print of a user is used as the biometric feature.

4. (Previously presented) A data carrier for authenticating a user of the data carrier for authorized use of the data carrier and for authenticating a data carrier terminal for accessing the data carrier, comprising a first memory area in which a secret code is stored such that the secret code can be read and decrypted and displayed only by an authorized data carrier terminal to authenticate the data carrier terminal for accessing the data carrier, and a second memory area in which data are stored which serve to authenticate the user for authorized use of the data carrier.

5. (Previously presented) A data carrier according to claim 4, wherein a PIN is stored in a third memory area.

6. (Previously presented) A data carrier according to either of claims 4 and 5, wherein the biometric data are generated by a fingerprint.

7. (Previously presented) An authentication system comprising a data carrier with memory areas and a data carrier terminal for accessing the memory areas of the data carrier, wherein

the data carrier has a first memory area for storing a secret code and a second memory area for storing biometric data,

the data carrier terminal has a first device which is authorized for reading the secret code from the first memory area and for decrypting the read secret code and for presenting the read secret code on a display, and a second device for reading biometric data of a biometric feature presented by a user, and

a device for comparing the read biometric data with biometric data stored in the second memory area in the data carrier and/or in the terminal.

8. (Previously presented) An authentication system according to claim 7, wherein the data carrier has a third memory area for storing a PIN.

9. (Previously presented) An authentication system according to claim 7 or 8, wherein the stored biometric data are generated by a fingerprint.